AMENDMENTS TO THE CLAIMS:

This listing of claims will replace, without prejudice, all prior versions, and listings, of the claims in the application:

Listing of Claims:

1-4. (Canceled)

5. (Currently amended) A ~~The~~ user device ~~of claim 4~~ for accessing information comprising an authentication system for certifying that the user of the device is the authorized user, the authentication system comprising:

a reader on the user device for sensing and reading a fingerprint of a user;

a memory for storing an authorized fingerprint on the user device;

a comparator on the user device, responsive to the reader and memory, for comparing the read fingerprint to the stored fingerprint;

a pseudo-random generator on the user device, responsive to the comparator, for generating a pseudo-random personal identification number (PIN) in accordance with a user specific algorithm when the read fingerprint and the stored fingerprint are equivalent; and

a display on the user device for displaying said PIN, said PIN being forwarded by said user to an issuer of said user device which grants access to said information;

wherein said issuer receives said PIN at an issuer network that comprises:

a customer database having customer information for a plurality of users;

an issuer pseudo-random generator, responsive to said customer database, for generating a pseudo-random customer code, wherein said customer code is generated in accordance with said user specific algorithm, and an issuer comparator, coupled to said customer database and said issuer generator, for comparing said customer code to said PIN, wherein the user is authorized and the device activation verified to access information when said customer code is equivalent to said PIN.

6. (Previously presented) The user device of claim 5, which is a card readable by a standard credit card reader.

7. (Previously presented) The user device of claim 5, which is a smart card.

8. (Previously presented) The user device of claim 5, which is a keyfob.

9-12. (Canceled)

13. (Previously presented) A method for verifying that a user of a device is an authorized user in order to access information, the method comprising:

sensing and reading a fingerprint of a user of the device;

comparing the read fingerprint with a fingerprint of the authorized user stored on the device;

generating a pseudo-random personal identification number (PIN) in accordance with a user specific algorithm when said read fingerprint is equivalent to the stored fingerprint, said PIN being used to verify activation of said device for accessing information;

displaying said PIN to said authorized user on said device;

transmitting said PIN to an issuer of said device;

generating a pseudo-random customer code in response to the receipt by said issuer of said PIN;

comparing said customer code to said PIN; and

verifying said user and activation of said device for accessing information when said customer code is equivalent to said PIN;

wherein said issuer grants access to said information when said PIN is equivalent to an issuer generated code.

14. (Original) A system wherein an authorized user can access information through an access device issuer comprising:

an access device, including an authentication system for verifying that a user of the device is the authorized user, wherein the authentication system comprises:

a reader for sensing and reading a fingerprint of a user;

a memory for storing an authorized fingerprint;

a comparator, responsive to the reader and memory, for comparing the read fingerprint to the stored fingerprint; and

a pseudo-random generator, responsive to the comparator, for generating a pseudo-random personal identification number (PIN) in accordance with a user specific algorithm when the read fingerprint and the stored authorized fingerprint are equivalent, wherein the user uses the generated PIN to verify activation of the card for accessing information; and

an issuer network for receiving said PIN from said user, wherein the network comprises:

a customer database having customer information for a plurality of users;

an issuer pseudo-random generator, responsive to said customer database, for generating a pseudo-random customer code, said customer code generated in accordance with said user specific algorithm; and

an issuer comparator, coupled to said customer database and said issuer generator, for comparing said customer code to said PIN, wherein said user and activation of said device for accessing information is verified when said customer code is equivalent to said PIN.

15-20. (Canceled)